

## **REMARKS**

This paper is filed in response to the non-final Office Action dated May 6, 2010. Claims 1-49 are pending in the instant application and stand rejected by the examiner. Claims 1, 3, and 39 are amended. New claims 50 and 51 are added herein. Reconsideration is respectfully requested in light of the amendments and remarks contained herein.

### ***Claim Rejections – 35 U.S.C. § 112***

Claim 3 is rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 3 has been amended to recite “the outgoing message comprises an attachment...” as the examiner suggests on page 2 of the office action. Thus, it is respectfully requested that the § 112 rejection of claim 3 be withdrawn.

### ***Claim Rejections – 35 U.S.C. § 101***

Claims 1-49 are rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Independent claim 1 is amended to recite “a processor-implemented method” and “a processor.” It is respectfully submitted that the amendment clarifies that the method is directed to statutory subject matter. Thus, it is respectfully requested that the § 101 rejections of claim 1 and claims that depend upon claim 1 be withdrawn.

Independent claim 39 is amended to recite “a processor-implemented system,” “a message store including a computer-readable memory,” and “a messaging client including a processor.” It is respectfully submitted that the amendment clarifies that

claim 39 is directed to statutory subject matter. Thus, it is respectfully requested that the § 101 rejections of claim 39 and claims that depend upon claim 39 be withdrawn.

### ***Claim Rejections – 35 U.S.C. §103***

Claims 1-8, 21-27, 33-34, and 39-48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Network Working Group RFC 2633 (June 1999) (Ramsdell) and in further view of Klein (U.S. Patent No. 6,496,853), and Baldonado (U.S. Patent No. 7,035,903). The remaining claims stand rejected under 35 U.S.C. § 103(a) based on Ramsdell, Klein, Baldonado, and one or more additional references. These rejections are respectfully traversed.

#### **Claim 1**

Claim 1 recites “wherein the message characteristics of the outgoing message are controlled *based on the content of the outgoing message.*” However, the Office mistakenly characterized this feature as “wherein the message characteristics of the outgoing message are controlled based on the outgoing message being related to a previously-received message.” Office Action, page 7, lines 11-12. Assignee respectfully disagrees with this characterization of claim 1’s feature. The feature of claim 1 does not recite that wherein the message characteristics of the outgoing message are controlled based on *the outgoing message being related to a previously-received message* as the Office characterizes. Instead, claim 1 recites that wherein the message characteristics of the outgoing message are controlled *based on the content of the outgoing message.* There is no mentioning in claim 1 that the message characteristics of the outgoing message are controlled based on the outgoing message being related to a previously-received message.

The Office cites to pg. 10, section 2.7.1.2 Rule 2 of Ramsdell as disclosing this feature of claim 1. The cited portion of Ramsdell reads:

2.7.1.2 Rule 2: Unknown Capabilities, Known Use of Encryption

If:

- the sending agent has no knowledge of the encryption capabilities of the recipient
- and the sending agent has received at least one message from the recipient,
- and the last encrypted message received from the recipient had a trusted signature on it,

then the outgoing message **SHOULD** use the same encryption algorithm as was used on the last signed and encrypted message received from the recipient.

It is respectfully submitted that the cited portion of Ramsdell does not disclose the feature of claim 1, “wherein the message characteristics of the outgoing message are controlled *based on the content of the outgoing message.*” The cited portion of Ramsdell merely discloses using the same encryption algorithm based on what was used on the most recent encrypted message received (i.e., an *incoming* message) from a recipient to encrypt an outgoing message to the recipient. According to the cited disclosure of Ramsdell, the sending agent would send an outgoing message to a recipient using the same encryption algorithm as the last encrypted message received from the recipient, no matter what the content of the outgoing message was. There is no disclosure in Ramsdell about controlling the message characteristics of the outgoing message *based on the content of the outgoing message.* Thus, Ramsdell does not disclose this claimed feature. The other cited references do not make up for Ramsdell’s deficiency. As such, it is respectfully requested that the § 103 rejection of claim 1 be withdrawn.

With respect to the other independent claim, claim 39 is amended to recite similar subject matter as claim 1. Accordingly, for similar reasons as offered for claim 1, claim 39 is allowable and should proceed to issuance.

#### **Claim 50**

The newly added claim 50 incorporates certain features of claims 22 and 23. An example of these features is shown at paragraph [0052] of the instant application. It is respectfully submitted that the cited references do not disclose the recited features of claim 50. In rejecting the features of claims 22 and 23 that are now incorporated into claim 50, the office cites to page 11, lines 23-33 of Ramsdell as disclosing selecting messaging settings associated with the first and second message characteristics if the first and second message characteristics do not include conflicting message characteristics. The cited portion of Ramsdell states:

If a sending agent is composing an encrypted message to a group of recipients *where the encryption capabilities of some of the recipients do not overlap, the sending agent is forced to send more than one message*. It should be noted that if the sending agent chooses to send a message encrypted with a strong algorithm, and then send the same message encrypted with a weak algorithm, someone watching the communications channel may be able to learn the contents of the strongly-encrypted message simply by decrypting the weakly-encrypted message.

The cited portion of Ramsdell discusses a situation where the sending agent must send more than one outgoing message where encryption capabilities of multiple recipients do not overlap. This is in stark contrast to selecting one set of messaging settings of the first and second message to control the characteristics of the outgoing message based on whether the settings are conflicting and based on the content of the

outgoing message as recited by claim 50. The other cited references do not make up for Ramsdell's deficiency. As such, it is respectfully requested that claim 50 be allowed.

**Claim 51**

The newly added claim 51 recites the selected messaging settings associated with the message characteristics of the received message are used to control message characteristics of any subsequent outgoing messages related to the received message. The amendment has support throughout the specification, including paragraph [0052]. It is respectfully submitted that the cited references, individually or in combination, do not disclose this feature.

The relevant portion of Ramsdell, pg. 10, lines 28-40, cited by the Office as disclosing the selecting step of claim 1, teaches using the encryption algorithm of the ***most recent*** received message to encrypt an outgoing message. After sending an outgoing message to the sender, new encrypted messages may be received from the sender before sending another outgoing message to the sender. The encryption algorithm of the last received message may be different from that of the previously received message. Thus, for each outgoing message, Ramsdell's approach requires a searching of a most recent encrypted message from the sender and a determination of the encryption algorithm of the most recent encrypted message. Ramsdell teaches away from using the encryption algorithm of one received message to control all subsequent messages related to the received message as required by claim 51. Other cited references do not make up for Ramsdell's deficiency. Because the combination of the cited references does not disclose the features of claim 51, it is respectfully requested that claim 51 be allowed.

It is noted that the assignee has not presented arguments herein with respect to the other dependent claims in the instant application. This is done without prejudice to the assignee's right to present arguments regarding each of the dependent claims at any point in the future. Further, since all of the dependent claims in the instant application depend from independent claims that are patentable over the cited references, the dependent claims are themselves patentable for at least the reasons set forth with respect to the independent claims.

### **CONCLUSION**

For the foregoing reasons, the assignee respectfully submits that the pending claims are allowable. Therefore, the assignee respectfully requests that the examiner pass this case to issuance.

Respectfully submitted,

/Matthew W. Johnson//

Matthew W. Johnson  
Reg. No. 59,108  
JONES DAY  
500 Grant Street, Suite 4500  
Pittsburgh, PA, USA, 15219-2514  
(412) 394-9524 (Direct)  
(412) 394-7959 (Fax)  
Attorneys for Assignee